IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND
SOUTHERN DIVISION

JOSIAH TRAGER, individually and on behalf of all others similarly situated, 809 Creekside Drive, Mount Pleasant, South Carolina 29464 Plaintiff, v. MARRIOTT INTERNATIONAL, INC. 10400 Fernwood Road Bethesda, Maryland 20817 (Montgomery County) Defendant.	**Civil Action No.: 1:18-cv-03745** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Josiah Trager brings this Class Action Complaint against Defendant Marriott International, Inc. ("Defendant" or "Marriott"), individually and on behalf of all others similarly situated, and complains and alleges upon personal knowledge as to himself and his own acts and experiences and, as to all other matters, upon information and belief, including investigation conducted by his attorneys.

I. NATURE OF THE ACTION

1. Plaintiff brings this class action against Marriott for its failure to secure and safeguard its customers' personal identifying information ("PII"), including names, mailing addresses, phone numbers, email addresses, passport numbers, rewards account information, date of birth, gender, arrival and departure information, reservation date, communication preferences, and credit and debit card information.

2. Marriott is one of the largest hotel chains in the World. Upon information and belief, approximately 500 million people, including Plaintiff, have stayed at Marriott and Marriott-owned properties and/or provided their PII to Marriott for safekeeping since 2014.

3. This case involves the data breach Marriott announced on November 30, 2018, wherein the PII of up to 500 million guests, again including Plaintiff, was exposed due to correctable flaws in Marriott's reservation system and database systems that, upon information and belief, have been ongoing for *at least four years*, since 2014 or earlier, which allowed hackers and other nefarious actors to take over guests' accounts and abscond with PII for demonstrably illegal purposes.

4. Marriott's security failures enabled the data thieves to steal Plaintiff's and the Class members' PII, putting Plaintiff's and Class members' financial information and interests at serious, immediate, and ongoing risk and, additionally, causing costs and expenses to Plaintiff and Class members from time spent and the loss of productivity in taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the theft of their PII, and the resulting stress, nuisance, and annoyance.

5. This Class Action Complaint is filed on behalf of all persons (or, in the alternative, all residents of South Carolina) whose PII was compromised in the data breach.

II. JURISDICTION AND VENUE

6. This Court has original jurisdiction pursuant to 28 U.S.C. § 1332(d)(2). In the aggregate, Plaintiff's claims and the claims of the other members of the Class exceed $5,000,000 exclusive of interest and costs, and Plaintiff and numerous Class members are citizens of States other than Defendant's state of citizenship.

7. This Court has personal jurisdiction over Marriott because Marriott has its principal place of business in Maryland and is therefore "at home" in the State of Maryland. Marriott also conducts substantial business throughout Maryland.

8. Venue is proper in this District pursuant to 28 U.S.C. §§ 1301(a)(2), 1391(b)(2), and 1391(c)(2) as a substantial part of the events and/or omissions giving rise to the claims emanated from activities within this District, and Marriott conducts substantial business in this District.

III. PARTIES

Plaintiff Josiah Trager

9. Plaintiff Josiah Trager is a resident of the State of South Carolina. Plaintiff has been a Marriott Rewards member since at least 2008 and a member of Starwood's Preferred Guest Loyalty Program since at least 2012.[1] Plaintiff's PII was stolen as a result of the unauthorized access detailed in this complaint.

10. Since the time the breach began in or around 2014, Plaintiff has had numerous instances of fraud on multiple credit cards linked to his Marriott account. Most recently, Plaintiff identified fraudulent charges of $432.17 at "Hanes.com" on December 2, 2018, and a fraudulent charge of $217.75 at "Adidas.com" on November 30, 2018, on two separate credit cards linked to his Marriott account, both of which were used for stays at Marriott-owned properties on dates prior to Marriott's announcement of the breach.

[1] Marriott acquired Starwood Hotels and Resorts Worldwide, LLC ("Starwood") on September 23, 2016. As part of its acquisition of Starwood, Marriott took control of Starwood's reservation system and the Starwood Preferred Guest loyalty program. The Starwood Preferred Guest loyalty program collected the PII of Starwood's guests. Marriott maintained the Starwood Preferred Guest loyalty program separately until August 18, 2018, when it was combined with Marriott's existing customer loyalty program (Marriott Rewards). Thereafter, Marriott continued to maintain the PII collected through the Starwood Preferred Guest loyalty program.

11. As a result of these charges, Plaintiff has expended considerable time and energy tracking his credit reports and account information, canceling and applying for replacement cards, filing a police report, and providing signed and notarized affidavits regarding the fraud he suffered.

Defendant Marriott

12. Defendant Marriott International, Inc. is a Delaware corporation with its principal place of business at 10400 Fernwood Rd, Bethesda MD 20817 (Montgomery County).

IV. FACTUAL BACKGROUND

The Data Breach

13. Marriott is a multinational hospitality company that manages and franchises a broad portfolio of hotels and related lodging facilities and is considered the largest hotel chain in the world, with more than 6,500 properties in 127 countries and territories globally, totaling over 1.2 million rooms.

14. Upon information and belief, Marriott collects, stores, and maintains the PII of all guests who stay at Marriott properties.

15. At some time before September 8, 2018, and possibly going back four years to 2014 or earlier, unauthorized actors accessed, copied, and "took steps toward[] removing" what appears to be the entirety of Marriott's guest reservation database.[2] Marriott disclosed that this included information for up to 500 million users.

16. Marriott discovered the ongoing breach on or about September 8, 2018, but did not notify the public of this information until almost three months later on November 30, 2018.[3]

[2] *See* http://news.marriott.com/2018/11/marriott-announces-starwood-guest-reservationdatabase-security-incident/.

[3] *Id.*

17. Marriott disclosed that for 327 million of these users, more detailed PII was stolen, including payment card numbers and expiration dates, purportedly in encrypted form. However, Marriott also stated that both components needed to decrypt the payment card information may have also been taken.[4]

18. According to Marriott's public statements, the only PII that was encrypted was its guests' payment card information. All other PII that was stolen was therefore not encrypted.[5]

19. The fact that Marriott believes its encryption key may also have been stolen indicates that Marriott did not store its encryption key in a cryptographic vault, as is required under standard data security best practices.[6]

20. Though Marriott was aware of the importance of maintaining proper control over the security of its guests' PII and of the likelihood of thieves trying to steal it, it failed to do so. Indeed, the hospitality industry has been targeted by data thieves repeatedly, with the Intercontinental Hotels Group, Hyatt, and Kimpton Hotels all having seen high-profile breaches in the last three years.

21. Noted cybersecurity expert Brian Krebs observed that "even the web site used to disclose this breach can't be bothered to use [a secure website]. These may seem like little things, but they are very public things. Makes you wonder what it looks like on the inside."[7]

Marriott Did Not Properly Safeguard Its Guests PII

22. In addition to the best practices cited above, both federal and state governments have established security standards and issued recommendations to temper data breaches and the

[4] *Id.*

[5] *Id.*

[6] *See, e.g.*, https://www.owasp.org/index.php/Key_Management_Cheat_Sheet#Storage.

[7] *See* https://twitter.com/briankrebs/status/1068505635556376576.

resulting harm to consumers and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[8]

23. In 2016, the FTC updated its publication, "Protecting Personal Information: A Guide for Business," which established guidelines for fundamental data security principles and practices for businesses.[9] The guidelines note businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

24. The FTC recommends that companies not maintain cardholder information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[10]

---

[8] *See* Federal Trade Commission, *Start With Security*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[9] *See* Federal Trade Commission, Protecting Personal Information: A Guide for Business, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personalinformation.pdf.

[10] *See* fn. 8, above.

25. The FTC has even brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45.

26. Marriott's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

27. Despite understanding the consequences of inadequate data security, Marriott failed to take appropriate protective measures to protect and secure guests' and customer's PII, including Plaintiffs and Class members; operated computer network systems with outdated operating systems and software; failed to enable point-to-point and end-to-end encryption; failed to detect intrusions dating back as far as 2014; and, failed to take other measures necessary to protect its data network.

Security Breaches Lead to Identity Theft

28. The United States Government Accountability Office noted *more than ten years ago*, in a June 2007 report on Data Breaches ("GAO Report"), that identity thieves use PII to open financial accounts, receive government benefits, and incur charges and credit in a person's name.[11] As the GAO Report states, this type of identity theft is the most harmful because it may take some time for the victim to become aware of the theft and can adversely impact the victim's credit rating. In addition, the GAO Report states that victims of identity theft will face

[11] *See* http:///www.gao.gov/new.items/d07737.pdf.

"substantial costs and inconveniences repairing damage to their credit records . . . [and their] good name."

29. According to the Federal Trade Commission ("FTC"), identity theft wreaks havoc on consumers' finances, credit history, and reputation, and can take time, money, and patience to resolve.[12] Identity thieves use stolen PII for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[13]

30. A person whose PII has been compromised may not see any signs of identity theft for *years*. According to the GAO Report:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

31. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for a number of years.[14] As a result of recent large-scale data breaches, identity thieves and cyber

[12] *See Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (2012), http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf (last visited December 5, 2018).

[13] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number. *Id*.

[14] Companies, in fact, also recognize PII as an extremely valuable commodity akin to a form of personal property. For example, Symantec Corporation's Norton brand has created a software application that values a person's identity on the black market. Risk Assessment Tool, Norton 2010, www.everyclickmatters.com/victim/assessment-tool.html. *See also* T. Soma, ET AL, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009).

criminals have openly posted stolen credit card numbers and other PII directly on various Internet websites, making the information publicly available, just as they have done here.

32. As documented above, Plaintiff has already been subject to precisely such fraud on numerous occasions as a result of Marriott's breach.

The Monetary Value of Privacy Protections

33. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information as follows:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[15]

34. Though Commissioner Swindle's remarks are more than a decade old, they are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a $26 billion per year online advertising industry in the United States.[16]

35. The FTC has also recognized that consumer data is a new – and valuable – form of currency. In a recent FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point by observing:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis – and profit.[17]

---

[15] *The Information Marketplace: Merging and Exchanging Consumer Data*, http://www.ftc.gov/bcp/workshops/infomktplace/transcript.htm (last visited December 5, 2018).

[16] *See Web's Hot New Commodity: Privacy*, http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html (last visited December 5, 2018) ("Web's Hot New Commodity: Privacy").

[17] *Statement of FTC Commissioner Pamela Jones Harbour* (Remarks Before FTC Exploring Privacy Roundtable), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf (last visited December 5, 2018).

36. Recognizing the high value that consumers place on their PII, many companies now offer consumers an opportunity to sell this information to advertisers and other third parties. The idea is to give consumers more power and control over the type of information that they share – and who ultimately receives that information. And, by making the transaction transparent, consumers will make a profit from the surrender of their PII.[18] This business has created a new market for the sale and purchase of this valuable data.[19]

37. Consumers place a high value not only on their PII, but also on the *privacy* of that data. Researchers have already begun to shed light on how much consumers value their data privacy – and the amount is considerable. Indeed, studies confirm that "when [retailers'] privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[20]

38. When consumers were surveyed as to how much they valued their personal data in terms of its protection against improper access and unauthorized secondary use – two concerns at issue here – they valued the restriction of improper access to their data at between $11.33 and $16.58 per website, and prohibiting secondary use at between $7.98 and $11.68 per website.[21]

39. Given these facts, any company that transacts business with a consumer and then compromises the privacy of that consumer's PII, like Marriott, has deprived that consumer of the full monetary value of the consumer's transaction with the company.

---

[18] *You Want My Personal Data? Reward Me for It*, http://www.nytimes.com/2010/07/18/business/18unboxed.html (last visited December 5, 2018).

[19] *See supra,* fn.9.

[20] Hann et al., *The Value of Online Information Privacy: An Empirical Investigation* (Mar. 2003) at 2, *available at* http://www.comp.nus.edu.sg/~ipng/research/privacy.pdf (last visited December 5, 2018); Tsai, Cranor, Acquisti, and Egelman, *The Effect of Online Privacy Information on Purchasing Behavior*, 22(2) Information Systems Research 254, 254 (June 2011).

[21] *Id.*

Damages Sustained by Plaintiff and the Class

40. A portion of the services purchased from Marriott by Plaintiff and the Class necessarily included compliance with industry-standard measures with respect to the collection and safeguarding of PII, including their credit and debit card information. Because Plaintiff and the Class were denied privacy protections that they paid for and were entitled to receive, Plaintiff and the Class incurred actual monetary damages in that they overpaid for the services purchased from Marriott.

41. Plaintiff and the Class have suffered additional injury in fact and actual damages including monetary losses arising from unauthorized bank account withdrawals, fraudulent card payments, and/or related bank fees charged to their accounts.

42. After the breach, Marriott encouraged consumers to check their credit reports, place holds on their credit reports, and close any affected accounts. However, as explained above, fraudulent use of cards might not be apparent for years. Therefore, consumers must expend considerable time taking these precautions for years to come.

43. Though Marriott has offered one year of free enrollment in "WebWatcher," which monitors internet sites where PII is shared and generates alerts if evidence of the consumer's PII is found, as security blogger Brian Krebs notes, "credit monitoring services will do nothing to protect consumers from fraud on existing financial accounts – such as credit and debit cards – and they're not great at stopping new account fraud committed in your name." This is particularly true where, as here, the PII that was stolen also includes names, mailing addresses, phone numbers, email addresses, passport numbers, rewards account information, date of birth, gender, and other identifying information.

44. As a result of these activities, Plaintiff and the Class suffered and will suffer additional damages arising from the costs associated with identity theft and the increased risk of identity theft caused by Defendant's wrongful conduct, particularly given the incidents of actual misappropriation from Plaintiff's financial accounts.

45. Plaintiff and the Class suffered and will suffer additional damages based on the opportunity cost and value of time that Plaintiff and the Class have been forced to expend, and will be forced to expend going forward, to monitor their financial and bank accounts as a result of the breach.

V. CLASS ACTION ALLEGATIONS

46. Plaintiff brings Counts I and II, as set forth below, on behalf of himself and as a class action, pursuant to the provisions of Rule 23 of the Federal Rule of Civil Procedure on behalf of a class defined as:

> All persons whose PII was accessed, compromised, or stolen from Marriott as a result of the Data Breach (the "General Class").

Excluded from the Class are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded are any judicial officers presiding over this matter and the members of their immediate families and judicial staff.

47. Plaintiff brings Count III, as set forth below, on behalf of himself and as a class action, pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure on behalf of a class defined as:

> All persons residing in the State of South Carolina whose PII was accessed, compromised, or stolen from Marriott as a result of the Data Breach (the "South Carolina Class").

Excluded from the South Carolina Class are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded are any judicial officers presiding over this matter and the members of their immediate families and judicial staff.

48. The General Class and South Carolina Class are collectively referred to as the "Class," unless specifically indicated otherwise.

49. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of his claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

50. **Numerosity – Federal Rule of Civil Procedure 23(a)(1).** The members of the Class are so numerous that their individual joinder herein is impracticable. On information and belief, Class members number in the hundreds of millions. The precise number of Class members and their addresses are presently unknown to Plaintiff but may be ascertained from Defendant's books and records. Class members may be notified of the pendency of this action by mail, email, Internet postings, and/or publication.

51. **Commonality and Predominance – Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** Common questions of law and fact exist as to all Class members and predominate over questions affecting only individual Class members. Such common questions of law or fact include:

a. Whether Marriott failed to use reasonable care and commercially reasonable methods to secure and safeguard its customers' PII;

b. Whether Marriott properly implemented its purported security measures to protect customer PII from unauthorized capture, dissemination, and misuse;

c. Whether Marriott's conduct constitutes breach of an implied contract;

d. Whether Marriott's conduct constitutes consumer fraud; and

e. Whether Plaintiff and the other members of the Class are entitled to damages, injunctive relief, or other equitable relief.

52. Marriott engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of himself and the other Class members. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action.

53. **Typicality – Federal Rule of Civil Procedure 23(a)(3).** Plaintiff's claims are typical of the claims of the other Class members because, among other things, all Class members were comparably injured through Defendant's uniform misconduct described above and were thus all subject to the data breach alleged herein. Further, there are no defenses available to Marriott that are unique to Plaintiff.

54. **Adequacy of Representation – Federal Rule of Civil Procedure 23(a)(4).** Plaintiff is an adequate Class representative because his interests do not conflict with the interests of the other Class members he seeks to represent, he has retained counsel competent and experienced in complex class action litigation, and he will prosecute this action vigorously. The Class's interests will be fairly and adequately protected by Plaintiff and his counsel.

55. **Insufficiency of Separate Actions – Federal Rule of Civil Procedure 23(b)(1).** Absent a representative class action, members of the Class would continue to suffer the harm described herein, for which they would have no remedy. Even if separate actions could be brought by individual consumers, the resulting multiplicity of lawsuits would cause undue hardship and expense for both the Court and the litigants, as well as create a risk of inconsistent

rulings and adjudications that might be dispositive of the interests of similarly situated purchasers, substantially impeding their ability to protect their interests, while establishing incompatible standards of conduct for Marriott. The proposed Class thus satisfies the requirements of Fed. R. Civ. P. 23(b)(1).

56. **Declaratory and Injunctive Relief – Federal Rule of Civil Procedure 23(b)(2).** Marriott has acted or refused to act on grounds generally applicable to Plaintiff and the other Class members, thereby making appropriate final injunctive relief and declaratory relief, as described below, with respect to the members of the Class as a whole.

57. **Superiority – Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff and the other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Marriott, so it would be impracticable for Class members to individually seek redress for Defendant's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation would create a potential for inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

VI. CLAIMS ALLEGED

COUNT I
Negligence
(On Behalf of the General Class)

58. Plaintiff incorporates paragraphs 1-57 as if fully set forth herein.

59. Defendant solicited and took possession of the PII of Plaintiff and the Class and had a duty to exercise reasonable care in securing that information from unauthorized access or disclosure. Defendant also had a duty to timely notify Plaintiff and the Class that their PII had been or may have been stolen. Defendant further had a duty to destroy the PII of Plaintiffs and members of the Class within an appropriate amount of time after it was no longer required by Marriott, in order to mitigate the risk of such non-essential PII being compromised in a data breach.

60. Defendant's duties arose from its relationship to Plaintiff and Class members and from industry custom and practice

61. Marriott breached these duties owed to Plaintiff and the other members of the Class by failing to take reasonable measures to safeguard their PII.

62. Plaintiff and the Class members would not have entrusted their private and confidential financial and personal information to Defendant in the absence of such duties.

63. Plaintiff and the other Class members suffered and will continue to suffer damages as a result of Defendant's breach of those duties. including but not limited to loss of their financial information and loss of time, money, and costs incurred as a result of increased risk of identity theft, all of which have ascertainable value to be proven at trial.

COUNT II
Breach of Implied Contract
(on Behalf of the General Class)

64. Plaintiff incorporates paragraphs 1-63 as if fully set forth herein.

65. Plaintiff and members of the Class reasonably believed that in providing PII to Defendant in exchange for the ability to reserve hotel rooms and guest services and to accrue loyalty program points, their PII would be protected with adequate security measures. This transaction created an implied agreement with Defendant that the PII provided would be safeguarded as one of Defendant's obligations under the agreement.

66. Plaintiff and members of the Class would not have provided Defendant with their PII in the absence of the implied agreement that Defendant would protect such information.

67. Plaintiff and members of the Class fully performed their obligations under their implied agreements with Defendant.

68. Defendant breached its implied agreement with Plaintiffs and members of the Class to protect their PII by (1) failing to implement security measures designed to prevent this breach; (2) failing to employ sufficient security protocols to detect the unauthorized network activity; (3) failing to maintain basic security measures such as reasonably segregating its encryption keys so that if data were stolen it would be unreadable or unusable; and (4) failing to provide timely and accurate notice to Plaintiff and members of the Class that their PII was accessed and compromised through the data breach.

69. Defendant's failure to properly secure the PII and notify Plaintiff and members of the Class about the breach is the direct and proximate cause of the damages Plaintiff and the Class have suffered and will suffer.

70. Plaintiff and members of the Class have been damaged by Defendant's breach of its implied agreement because their PPI has been compromised and they are at increased risk of future identity theft. Plaintiff and members of the Class have also been deprived of the value of their PII and have lost money and property as a result of Defendant's unlawful and unfair conduct.

COUNT III
Violation of the South Carolina Data Breach Notification Law
(On Behalf of the South Carolina State Class)

71. Plaintiff incorporates paragraphs 1-70 as if fully set forth herein.

72. Section 39-1-90(A) of the South Carolina Code of Laws mandates that any entity conducting business in that State, as Marriott was and is here, "shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of this State whose personal identifying information that was not rendered unusable through encryption, redaction, or other methods was, or is reasonably believed to have been, acquired by an unauthorized person when the illegal use of the information has occurred or is reasonably likely to occur or use of the information creates a material risk of harm to the resident." Such disclosure "must be made in the most expedient time possible and without unreasonable delay." In addition, Section 39-1-90(B) directs that "[a] person conducting business in this State and maintaining computerized data or other data that includes personal identifying information that the person does not own shall notify the owner or licensee of the information of a breach of the security of the data *immediately following discovery*, if the personal identifying information was, or is reasonably believed to have been, acquired by an unauthorized person" (emphasis added).

73. Marriott violated Section 3-1-90 by failing to provide Plaintiff and members of the South Carolina Class with any notice whatsoever of the breach until November 30, 2018, nearly three months after it claims to have discovered the breach on September 8, 2018.

74. Marriott's failure to comply with its notification requirements under South Carolina law was willful and knowing.

75. Accordingly, Plaintiff and members of the South Carolina Class have suffered, and seek to recover, actual damages, statutory damages, and attorneys' fees and costs.

VII. DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury of all claims in this complaint so triable.

VIII. REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the other members of the Class proposed in this Complaint, respectfully requests that the Court enter judgment in his favor and against Marriott, as follows:

A. Declare that this action is a proper class action, certifying the Class(es) as requested herein, designating Plaintiff as Class Representative and appointing the undersigned counsel as Class Counsel for the Class;

B. Order Marriott to pay actual damages to Plaintiff and the other members of the Class;

C. Order Marriott to pay for not less than three years of credit card monitoring services for Plaintiff and the other members of the Class;

D. Order Marriott to pay punitive damages, as allowable by law, to Plaintiff and the other members of the Class;

E. Order Marriott to pay statutory damages to Plaintiff and the other members of the South Carolina Class;

F. Order Marriott to disseminate individualized notice of the Security Breach to all Class members and to post notice of the Security Breach in all of its affected properties;

G. Order Marriott to pay attorneys' fees and litigation costs to Plaintiff and the other members of the Class;

H. Order Marriott to pay both pre- and post-judgment interest on any amounts awarded; and

I. Order such other and further relief as may be just and proper.

JURY TRIAL DEMAND

Plaintiff demands a trial by jury on all questions of fact.

Dated: December 5, 2018

Respectfully submitted,

Andrew D. Freeman (Fed. Bar No. 03867)
Neel K. Lalchandani (Fed. Bar No. 20291)
BROWN, GOLDSTEIN & LEVY, LLP
120 E. Baltimore Street, Suite 1700
Baltimore, MD 21202
Tel.: (410) 962-1030
Fax: (410) 385-0869
adf@browngold,com
nlalchandani@browngold.com

Bruce D. Greenberg (pro hac vice forthcoming)
LITE DEPALMA GREENBERG, LLC
570 Broad Street, Suite 1201
Newark, New Jersey 07102
Phone: (973) 623-3000
bgreenberg@litedepalma.com

Katrina Carroll (pro hac vice forthcoming)
Kyle A. Shamberg (pro hac vice forthcoming)
LITE DEPALMA GREENBERG, LLC
111 W. Washington Street
Suite 1240
Chicago, Illinois 60602
312.750.1265
kcarroll@litedepalma.com
kshamberg@litedepalma.com

Joseph LoPiccolo (pro hac vice forthcoming)
John N. Poulos (pro hac vice forthcoming)
POULOS LOPICCOLO PC
1305 South Roller Road
Ocean, New Jersey 07712
732-757-0165
lopiccolo@pllawfirm.com
poulos@pllawfirm.com

Counsel for Plaintiff and Putative Class